REMARKS

Claims 1-26 remain in the application for consideration. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application.

§§ 102 Rejections

Claims 1-26 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,052,468 to Hillhouse (hereafter "Hillhouse").

Before undertaking a discussion regarding the substance of the Office's rejections, the following discussion of Hillhouse is included in order to assist the Office in appreciating the patentable distinctions between these references and the claimed subject matter in this application.

The Hillhouse Reference

Hillhouse discloses systems and methods for improving portability of secure encryption key data files by ***re-securing*** key data files according to different security processes for mobility. Specifically, Hill teaches a method of generating secure key databases that is portable to systems having different configurations. Hill also teaches a method of selecting a user authentication method from a plurality of user authorization methods ***for use in securing*** a key data file. Finally, Hill teaches a method of ***securing*** a key database with multiple security methods.

In accordance with Hill's teachings, a key data file comprises a secured cryptographic key which can be secured again according to an authentication method selected from a plurality of available authentication methods available to a

user on a particular system. Additionally, the key can be ***re-secured*** over and over again based on selected available authentication methods. The key data is then accessible only via the authentication method(s) used. Thus, the systems and methods in Hillhouse ***control access to key data files by securing a cryptographic key to that file.***

Applicant's Disclosure

Applicant's disclosure provides methods and arrangements for controlling access to resources in a computing environment. These methods and arrangements identify authentication mechanism(s) (and/or characteristics thereof) used in verifying a user to subsequently operating security mechanisms. Thus, additional control is provided by differentiating user requests based on this ***additional information.*** For example, in a computer capable of supporting multiple authentication mechanisms, at least one embodiment ***generaes an operating system representation*** of at least one identity indicator associated with at least one authentication mechanism, and subsequently ***controls access*** (to at least one resource) ***based on the operating system representation.*** In certain implementations, at least one security identifier that identifies the authentication mechanism in some way can be generated. In other implementations, the operating system representation is compared to at least one access control list (with at least one access control entry). Here, for example, the access control entry may specify whether the user authenticated (by the authentication mechanism) is permitted access to the resource.

Claims Rejected over Hillhouse under §§ 102

Claim 1 recites a method for use in a computer capable of supporting multiple authentication mechanisms comprising:

- generating at least one indicator associated with and identifying at least one authentication mechanism; and
- ***controlling access to at least one resource based on the indicator.***

In making the rejection, the Office argues that Hillhouse discloses generating at least one indicator associated with and identifying at least one authentication mechanism (citing column 8, lines 27-43) and controlling access to at least one resource based on the indicator (citing column 5, lines 32-38). Applicant respectfully disagrees and submits that the excerpt cited by the Office (column 5) merely discusses a method in which a key file comprising a cryptographic key (secured by a biometric authentication method) requires biometric authentication to access the cryptographic key. Nothing discloses or suggests ***controlling access to at least one resource based on a generated indicator which is associated with and identifies at least one authentication mechanism***. This excerpt is reproduced below:

> Referring to fig. 1, a prior art method of accessing secured data is shown for use in a network comprising a plurality of computers each having a biometric imaging means. A key data file comprises a cryptographic key, which is secured using a biometric authentication method. According to the method, biometric authentication is required to access the cryptographic key.

The excerpt cited by the Office neither discloses nor suggests the subject matter of this claim. Accordingly, for at least this reason, this claim is allowable.

Claims 2-10 depend from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither shown nor suggested by the reference of record either singly or in combination with one another.

Claim 11 recites a computer-readable medium for use in a device capable of supporting multiple authentication mechanisms, the computer-readable medium having computer-executable instructions for performing acts comprising:

- producing at least one indicator that uniquely identifies at least one authentication mechanism supported by the device; and
- causing the device to selectively ***control access to at least one resource*** operatively coupled to the device ***based at least in part on the indicator.***

In making the rejection, the Office argues that Hillhouse discloses generating at least one indicator associated with and identifying at least one authentication mechanism (citing column 8, lines 27-43) and controlling access to at least one resource based on the indicator. (citing column 5, lines 32-38). Applicant respectfully disagrees and submits that, as discussed above, the excerpt cited by the Office (column 5) does not disclose or suggest ***controlling access to at least one resource*** operatively coupled to the device ***based at least in part on a indicator that uniquely identifies at least one authentication mechanism supported by the device.***

The excerpt cited by the Office neither discloses nor suggests the subject matter of this claim. Accordingly, for at least this reason, this claim is allowable.

Claims 12-20 depend from claim 11 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 11, are neither shown nor suggested by the reference of record either singly or in combination with one another.

Claim 21 recites an apparatus comprising:

- at least one authentication mechanism configured to generate at least one indicator that identifies the authentication mechanism;
- an access control list;
- at least one access controlled resource; and
- logic operatively configured to compare the indicator with the access control list and selectively control access to the resource based on the indicator.

In making the rejection, the Office argues that Hillhouse discloses at least one authentication mechanism configured to generate at least one indicator that identifies the authentication mechanism (column 8, lines 27-43) and logic operatively configured to compare the indicator with the access control list and selectively control access to the resource based on the indicator. (citing 7, lines 1-26).

Applicant respectfully disagrees and submits that the excerpt cited by the Office (column 7) discusses a method for copying or porting encryption key data from one system to another. Specifically, "[t]he authentication method is selected from a plurality of available authentication methods. The user is authenticated according to the selected method and the secured cryptographic key is secured according to that method." (column 7, lines 6-10). Thus, in Hillhouse, an indicator of the authentication mechanism itself is not used to control access; rather access

to data by a user (or users) is determined simply by whether or not that user (or users) can adequately authenticate via the same means that the desired data is secured (and re-secured) by. Nothing discloses or suggests generating at least one ***indicator that identifies the authentication mechanism***, comparing the indicator with an access control list and selectively controlling access to the resource ***based on the indicator***.

The excerpt cited by the Office neither discloses nor suggests the subject matter of this claim. Accordingly, for at least this reason, this claim is allowable.

Claims 22-26 depend from claim 21 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 21, are neither shown nor suggested by the reference of record either singly or in combination with one another.

Conclusion

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 1/21/05

By: _____

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256